Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1701 01/02/15

~ North Korea Had Help? ~ People Are Talking! ~ PSN Back Online!
~ Gmail Blocked in China? ~ 2014, The Sad Internet! ~ NSA Eavesdropping!
~ Selling Unwanted Games? ~ Okay To Ruin Christmas? ~ Bing, Yahoo Outages!

~ Net Neutrality Pushback ~ Google Outs Windows 8.1 ~ Halo 5 Beta!

-* Lizard Squad Hacker Arrested *-
-* Lizard Squad Offers DDoS Attack Tool *-
-* U.S. Hits North Korea With Huge Sanctions! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Again, let me wish you all a Happy New Year! Believe it or not, this issue marks our 17th year! I honestly didn't think that we'd still be around for very long back in the 90's, much less this long! But, we're here. For how much longer, I have no idea. So, for the moment, let's welcome in the new year, and have a drink or three to celebrate!

Until next time...

=~=~=~=

->In This Week's Gaming Section - PS Network Back Online After 3-day Outage!
""""""""""""""""""""""""""""""" Alleged Lizard Squad Hacker Arrested!
Where To Sell Back Your Unwanted Games!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

PlayStation Back Online After 3-day Outage

Sony says its PlayStation Network is back online after three days of disruptions that began on Christmas.

But heavy traffic might continue to cause problems for customers seeking to play their favorite games, the company said Sunday.

A group of hackers called Lizard Squad or someone claiming to speak for it took credit for the disruptions. In a blog post Saturday night saying service had been restored, Sony vice president Catherine Jensen added that "PlayStation Network and some other gaming services were

attacked over the holidays with artificially high levels of traffic to disrupt connectivity and online gameplay."

Microsoft’s Xbox Live service, which also went down Thursday, was back online Friday, although the company reported continuing problems.

So far, there’s no evidence to link these episodes with last month’s attack on Sony Pictures Entertainment. The FBI has blamed that attack on North Korea, which was furious about Sony’s "The Interview," a movie comedy about a plot to assassinate North Korean leader Kim Jong Un.

Lizard Squad Member ’Ryan’ Explains Why It’s OK To Ruin Christmas

Millions of children and adults who expected to enjoy 25 December playing games on their Microsoft or Sony consoles were deprived of the chance by a Distributed Denial of Service attack (DDoS).

The attack, clearly timed to create the maximum amount of publicity and disruption, was directed at the PlayStation and Xbox servers the games consoles depend upon.

It prevented gamers from setting up their consoles, downloading games or joining others to play games online.

Although both networks are up and running again now Microsoft restored their service more than a whole day sooner than Sony - a final ignominy in a year to forget for them.

Hacking group Lizard Squad has claimed responsibility for the attack, having previously threatened both companies.

In an interview with Sky News a man speaking for the hackers claimed it was ’basically’ the work of three people and they’d done it...

...to raise awareness, to amuse ourselves...

They [Microsoft and Sony] should have more than enough funding to be able to protect against these attacks.

In the event it was a different kind of funding that satisfied their ’principles’.

Internet entrepreneur and console gamer Kim Dotcom engaged the vandals via Twitter on 26 December and offered them vouchers for his MegaPrivacy service worth $300,000 USD if they called off the attacks.

A tactic which worked, apparently.

Speaking from Finland the Lizard Squad front man, calling himself Ryan but named by Brian Krebs as Julius Kivimäki, told Sky’s Joe Tidy that he didn’t feel any guilt about depriving people of their Christmas presents:

I’d be rather worried if those people didn’t have anything better to do than play games on their consoles on Christmas Eve and Christmas Day.

I mean I can’t really ... feel bad. I might have forced a couple of kids to spend their time with their families instead of playing games.

Ryan’s attempt to justify the attack as somehow doing some good, whilst shifting the blame to the victims and passing off the impact on gamers as inconsequential, is a stuck record we’ve heard many times before.

This is not what helping looks like, this is doing it ’for the lulz’.

Ethical hackers, the kind who actually help improve security, use their skills to find bugs and report them quietly and responsibly so as to minimise collateral damage.

But a DDoS attack isn’t a skilful hack - it isn’t picking the lock, it’s blocking the door from the outside with as much rubbish as you can pile up.

You won’t see Lizard Squad earning bug bounties from Microsoft or appearing in Sony’s hall of thanks.

It isn’t for Lizard Squad, or anyone else, to decide how millions of people can or can’t spend their Christmas day.

And the gamers aren’t the only victims.

The attack itself was almost certainly launched from a large network of compromised computers that are owned and paid for by others. Computers that were broken into and used illegally and which have to remain compromised for groups like Lizard Squad to operate.

Lizard Squad aren’t interested in security, they’re in it for the lulz, and we know how that story ends.

Alleged Lizard Squad Hacker Arrested

One of the guys allegedly responsible for keeping you from playing video games on Christmas Day 2014 has been arrested.

On Monday (Dec. 29) United Kingdom police arrested Vinnie Omari, 22, alleged member of the hacking group known as Lizard Squad, while raiding his London home, the Daily Dot reports. Lizard Squad has claimed responsibility for the distributed denial-of-service (DDoS) attacks that knocked Xbox Live and the PlayStation Network offline on Dec. 25.

Omari’s arrest followed a raid on his home by the police. A press release from the Thames Valley Police Department, apparently concerning Omari, says that he was arrested "on suspicion of fraud by false representation and Computer Misuse Act offences [sic]." Omari was released from jail on Tuesday, and thus far no charges have been filed.

They took everything... Xbox One, phones, laptops, computer USBs, etc.," Omari said in an email to the Daily Dot, who broke the story. Omari also included a picture of the search warrant.

Lizard Squad has risen to notoriety in the past few months by claiming responsibility for some high-profile DDoS attacks against gaming networks. On Christmas Day, the group only stopped its attacks on Xbox Live and the PlayStation Network after MegaUpload founder Kim Dotcom gave the group 3,000 vouchers for his uploading service.

After that, Lizard Squad claimed the Christmas attacks were just a "commercial" for a do-it-yourself DDoS tool called Lizard Stresser, which the group was developing and offering for sale on the online black market.

On Dec. 27, Omari was interviewed by British news channel Sky News, where he was cited as a "computer security analyst" and talked about Lizard Squad's activities. Two days later, independent security reporter Brian Krebs claimed in a report posted to his blog that Omari was a member of Lizard Squad. In the same post, Krebs also claimed that the Lizard Squad member who sometimes uses the online pseudonym "Ry|an" was a Finnish teenager named Julius Kivimäki.

It seems the Federal Bureau of Investigation agrees with him; the FBI is also reportedly investigating a Lizard Squad member named "ryanc" or Ryan, whom they believe to be a Finnish teenager, as the Daily Dot reported on Dec. 28th. "Ryan" recently appeared on Sky News, openly claiming that he was a member of Lizard Squad.

"Both of these individuals [Omari and Kivimäki] may in fact be guilty of nothing more than taking credit for other peoples crimes. But I hope it s clear to the media that the Lizard Squad is not some sophisticated hacker group," Krebs wrote in his blog post, dated the same day as Omari's arrest.

Today, as news of Omari's arrest broke, Krebs seems to have had a laugh on Twitter, as he tweeted the photo of the search warrant with the words "Poor Vinnie ...#skidfail."

Halo 5 Beta Impressions, It s Alright But Needs Work

After the underwhelming release of 343 Industries Halo 4, the next numbered entry in the franchise, Halo 5: Guardians is set for release sometime this year. For those of you who own the Halo: Master Chief Collection on Xbox One, the beta is running from December 29, 2014 through January 18, 2015. As is usual, the beta is focused exclusively on the arena portion of the online multiplayer aspect of Halo 5: Guardians.

After downloading 10GB worth of Halo 5 goodness, it d be a lie to say my personal hopes for the beta were high. Halo 4 felt like an alternate-world Halo game, and the Master Chief Collection simply didn t work. Rejoice friends, for the beta is pretty damn enjoyable. According to 343 Industries, the beta is completely hosted on dedicated servers at 60fps. It certainly, shows. Matches were found quickly, and played often. Do keep in mind that this is a beta so lag and some disconnect issues are abound. but overall everything is far more stable than the Master Chief Collection.

The first thing I noticed about the arena portion of Halo 5 multiplayer, was the commitment to supplementing the story of Guardians. Before you even download the beta, you re greeted with a cinematic of a group of Spartan IVs standing behind the Arbiter and the Halo:Nightfall TV series lead, Agent Locke. The two discuss Master Chief, and reveal he s being hunted for going AWOL. It s Locke s duty to hunt down the Master Chief, and from the looks of it, the Arbiter is keen on helping, though he states that Master Chief must have his reasons. Whether or not these cinematics

play throughout an arena season has yet to be revealed, though like the Spartan Ops from Halo 4, this seems likely.

But enough of the story crap, let s get down to why you re here gameplay. Remember, these impressions are based on the first week of the beta, which includes one gametype: team slayer (team deathmatch) and two maps: Empire and Truth. As the beta progresses, 343 Industries promises to release new maps and gametypes with the next batch of content dropping on January, 2 2015.

First and foremost, Halo 5 is fast. Out of all the entries in the franchise, this one is all about traversal. The agile Spartan IV soldiers are nimble and squishy. They hit fast, but go down quick. As for traversal, players now have more options to them in combat helping them get into and out of firefights. Like Advanced Warfare these spartans have the ability to do a burst strafe using the thrusters on the back. This short burst allows them to slide around corners and get into cover, or traverse a gap their jump cant quite reach. This burst does come with a short cooldown limiting the ability to spam the maneuver.

The next addition to the game, and certainly my favorite, is the hover. When your character is aerial, aims down the sights of your weapon (which looks badass as hell) and you will hover in place for a few seconds. This move allows a tactical view of the area ahead, and helps give you the jump on unsuspecting enemies. Careful though, a space-age soldier hovering in the air just screams shoot me.

Sitting duck waiting to pounce

Another aerial maneuver is the ground pound. While in the air, clicking on both analog sticks and holding them breaks you out of the first-person perspective and give you a view of your character and the area below and allows you to control your landing reticule. After a few seconds, your thrusts build enough thrust to send you to the floor, plummeting like a comet and delivering a deadly pound to an unsuspecting foe. Hard to pull of, but cool nonetheless.

The final addition to the Halo 5 players arsenal is the sprint and shoulder charge. If you ve played any shooter, you know that clicking on the left analog stick allows your character to sprint for a short duration of time. In Halo 5 that sprint is indefinite. Hitting melee during a sprint will initiate a shoulder charge that helps to clear a short distance and damages any enemy in your path. This move is excellent for clearing space in a short-to-mid-range firefight, but as you might ve expected, leaves you vulnerable should you miss.

As for the maps themselves, Truth, the Halo 2 Midship remake, stands out on it s own as a gem. Although, the color palette of red and blue enemies left me squinting at times throughout the purple map. Empire on the other hand is a beautiful asymmetrical map with interesting spaces surrounding the power weapons. On Empire, the power weapons are the ol sniper rifle. One side of the map houses the sniper inside some tight quarters making for some tense hand-to-hand combat. The opposite side of the map places the sniper in an open area, encouraging teamwork to secure the item, and rewarding the winner with an open alley to snipe from.

A major gripe with the beta so far is the kill-cam. Kill-cams have a history they punish players who managed to find nice hiding spots. Additionally, the kill-cam as it stands simply doesn t work. Most of time, the only thing that shows is the time after you re killed,

rekindling the rage you felt when you first died. Followed by the familiar beep, beep, BEEEEEP of the respawn timer that takes you to a black screen before throwing you back into the action. But surely that is more of a server issue.

As for the most impressive aspect of the Halo 5 beta so far, the trophy has to go to the design aesthetics. The user interface is sleek, and positively Halo in vibe and sound. Even the Announcment of the respawn of the power weapons is a wonderful addition from Halo 4 that encourages teams to fight for their weapons.

Where To Sell Back Your Unwanted Games

We all get dud gifts for the holidays. And while you might appreciate the fact that Uncle Ernie tried his hardest to give you something special, that copy of The Voice: I Want You probably wasn t exactly what you were hoping for.

If you re lucky, Uncle Ernie knew he was out of his depth and included a gift receipt with the present. But even if he didn t, you have options. Mercifully. Here s what to do with games you re not planning on keeping:

The most popular and in most cases, quickest choice is to head to your local GameStop. The retailer is easy to find, and it ll take back pretty much any game.

GameStop will let you swap games for either cash or store credit, though you re a sucker if you take the cash. The company puts a much higher value on trades, and unless you re giving up the habit entirely, chances are you ll want a new game sooner or later.

If you re trading in several games or plan to trade in more through the course of the year, it s worth signing up for the PowerUp Rewards program. There s a $15 annual fee, but that increases the value of your trades, up to a couple of bucks per title. That can pay off in the long run if you re a big gamer.

Don t just trade games whenever the mood strikes you, though. Several times per year, the company offers promotions that put a bonus on trade-ins, which can boost their value by anywhere from 30 to 90 percent. The best way to keep up with that is by checking GameStop s flyers, its website, or the forums of sites like CheapAssGamer.

GameStop got some competition this year, though, as Walmart jumped into the trade-in business and came to play. In late October, the retailer launched its certified preowned program in 1,700 stores nationwide.

Walmart s trade program accepts games for all existing console systems, but unlike GameStop, the retailer does not accept game hardware. CE Exchange maintains the database determining the value of the titles. That eases the burden on Walmart associates, who only have to scan the game s UPC code (after first checking the disc for scratches and cracks) to determine how much credit to give the customer.

This isn t the first time Walmart has explored the used game business, but it s by far the largest expansion of the program. In 2009, the retailer launched a pilot program using kiosks but never expanded on it. This

time, it s a bit more serious.

Why choose Walmart over GameStop? It really boils down to the game. Before you head to either retailer, consider price shopping online. GameStop s site will give you an idea of how much it s paying for recent titles.

Walmart has a similar option as well. And both Best Buy and Target list their prices for all games online. You can get an extra 10 percent on your trades at Best Buy if you re a member of its Unlocked Gamers Club, though at $99 for a two-year membership, it s a bit pricey.

Stay home and head online?Of course, if you d just as soon have the cash, there s always eBay, though you ll be competing against a lot of people doing the same thing. Unless you re selling a limited edition or otherwise special copy of the game, the prices might not be so hot.

Alternate bidding site Glyde.com will also get you some cash. It s not as robustly populated as eBay, which can be a good or bad thing, depending on the game.

Interestingly, Amazon is now a big player in the used game space. Here s how it works: Enter the games you want to dispose of on the site and you ll see their trade value. Assuming that s acceptable to you, you print out a free shipping label, box them up, and drop them off at the nearest UPS location. A week or so later, your Amazon account will receive a credit in that amount, which can be used on games or anything else the site carries. Bad games for a new iPad? Not a bad trade.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

U.S. Suspects North Korea Had Help Attacking Sony Pictures

U.S. investigators believe that North Korea likely hired hackers from outside the country to help with last month’s massive cyberattack against Sony Pictures, an official close to the investigation said on Monday.

As North Korea lacks the capability to conduct some elements of the sophisticated campaign by itself, U.S. investigators are looking at the possibility that Pyongyang "contracted out" some of the cyber work, according to the official, who was not authorized to speak on the record about the investigation.

The attack on Sony Pictures is regarded to be the most destructive ever against a company on U.S. soil because the hackers not only stole huge quantities of data, but also wiped hard drives and brought down much of the studio’s network for more than a week.

While U.S. officials investigate whether North Korea enlisted help from

outside contractors, the FBI stood by its previous statement that Pyongyang was the prime author of the attack against the Sony Corp unit.

"The FBI has concluded the Government of North Korea is responsible for the theft and destruction of data on the network of Sony Pictures Entertainment," the Federal Bureau of Investigation said in a statement to Reuters.

"There is no credible information to indicate that any other individual is responsible for this cyber incident," the FBI said.

North Korea has denied that it was behind the Sony attack and has vowed to hit back against any U.S. retaliation.

The people who claimed responsibility for the hack have said on Internet postings that they were incensed by the film "The Interview," a Sony Pictures comedy about a fictional assassination of North Korean leader Kim Jong Un.

Some security experts have begun to question the FBI’s assertion that Pyongyang was behind the cyberattack. For instance, consulting firm Taia Global said the results of a linguistic analysis of communications from the suspected hackers suggest they were more likely from Russia than North Korea. Cybersecurity firm Norse said it suspects a Sony insider might have helped launch the attack.

"I think the government acted prematurely in announcing unequivocally that it was North Korea before the investigation was complete," said Mark Rasch, a former federal cybercrimes prosecutor. "There are many theories about who did it and how they did it. The government has to be pursuing all of them."

FBI Bulletin States Sony Hackers Are Targeting Media Outlets

The hacking organization that took credit for infiltrating Sony Pictures Entertainment and stealing 10 TB worth of data has also threatened at least one news media organization, according to an FBI bulletin that’s making the rounds in cyberspace. Known as the Guardians of Peace, or GOP, the group of hackers proved a major headache for Sony, who’s antics appear to have been motivated by The Interview, a comedy involving an assassination attempt against North Korean leader Kim Jong-un.

The bulletin, which is dated December 24, 2014 and is labeled as unclassified, said the threat against the unnamed news organization by the GOP "may extend to other such organizations in the near future." It was first picked up the The Intercept and has since been posted online.

In the bulletin, the FBI refers to Sony as "USPER1" and the unnamed "news media organization" as "USPER2," adding that the GOP posted Pastebin messages that specifically taunted the FBI and USPER2 for the quality of their investigations and implied an additional threat. According to the bulletin, no specific consequence was mentioned in the post.

News outlet Fox News said it was able to confirm with the FBI that the bulletin is real, however it’s being stressed that it doesn’t mean there’s any specific evidence of a threat to a news organization.

"As part of our ongoing public-private partnerships, the FBI and DHS routinely share information with the private sector and law enforcement community," the official said. "The FBI and DHS are not aware of any specific credible information indicating a threat to entertainment or news organizations, however, out of an abundance of caution, we will continue to disseminate relevant information observed during the course of our investigations."

The FBI in December blamed North Korea for the cyberattack against Sony, which may have been aided by an insider. North Korea maintains it had nothing to do with the incident.

U.S. Hits North Korea with Huge New Sanctions in Response to Sony Hack

The United States just struck back against North Korea for its alleged role in the hack of Sony Pictures. In official statement released on Friday, U.S. president Barack Obama said he was signing an executive order authorizing stiff sanctions against North Korea for its ongoing provocative, destabilizing, and repressive actions and policies, particularly its destructive and coercive cyber attack on Sony Pictures Entertainment.

Bloomberg reports that the order targets 10 individuals in North Korea along with three state agencies and effectively authorizes the Treasury Department to block the individuals and agencies from accessing the U.S. financial system and banning U.S. citizens from engaging in business with them.

Lizard Squad Offers $6 DDoS Attack Tool

Have a site you'd like to hit with a distributed denial-of-service (DDoS) attack? Lizard Squad has just the thing: a DDoS attack tool, which is now available starting at $5.99 per month.

The group, which took responsibility for the recent attack on the Xbox and PlayStation networks, is offering several packages for its Lizard Stresser product, payable via bitcoin, of course. They range from $6 per month (for 100 seconds) to $130 (for 30,000 seconds).

Some come with "lifetime" option, which really only covers the five-year expected lifespan of Lizard Stresser, according to the group's website (which we have not linked to); users can pay a one-time fee of $30 to $500.

There's even a referral system: You earn 10 percent of whatever money your friends spend. Also pick from Lizard Stresser's add-ons, for more website-takedown power.

According to VentureBeat, the site will soon accept payments via PayPal. The Lizard Squad has been busy lately. In addition to the PlayStation and Xbox attacks, it claims to have played a part in the Sony Pictures attack.

In an interview with The Washington Post, an alleged member of the Lizard Squad (identified only as "a Ryan Cleary," but not the same one who was

convicted of targeting the websites of the CIA and others) offered more details about the security breaches.

"[O]ne of our biggest goals is to have fun, of course," the hacker said. "But we're also exposing massive security issues with these companies people are trusting their personal information with. The customers of these companies should be rather worried."

Unlike the Sony Pictures hack, DDoS attacks typically just crash websites rather than allow for information leaks. Still, "Ryan Cleary" believes Sony and Microsoft's business-critical systems are not top security priorities.

"We told them almost a month before that we'd do this," he told the Post, referring to an early December tweet that promised a "Christmas present" for Microsoft. "And yet we had no difficulties dropping them."

But the collective may have dug its claws in even deeper: "Ryan Cleary" admitted to the newspaper that "we do know some people from the [Guardians of Peace]," which infiltrated Sony Pictures Entertainment.

When asked if the Lizard Squad was involved in the attack, the hacker brushed it off, saying, "we didn't play a large part in that." According to "Cleary," the group simply passed along some Sony employee logins to the GOP for their initial hack.

The Post also asked about Lizard Squad's latest target: Tor, which allows for anonymous and/or difficult-to-track activity on the Internet.

In a Friday tweet, Lizard Squad (or someone affiliated with it) clarified that "we are no longer attacking PSN or Xbox. We are testing our new Tor 0day."

Despite the message, "Cleary" said there is no actual zero-day attack (which exploits a previously unknown vulnerability). Instead, the hackers are running a huge volume of Tor nodes. As of Monday, he suggested Lizard Squad is in control of 50 percent of the overall Tor network, and more than 70 percent of exit nodes.

The goal, he explained, is simple: "make everyone understand how easy this flaw in Tor is to exploit."

In a Friday statement, however, the Tor Project said "the attackers have signed up many new relays in hopes of becoming a large fraction of the network. But even though they are running thousands of new relays, their relays currently make up less than 1 percent of the Tor network by capacity. We are working now to remove these relays from the network before they become a threat, and we don't expect any anonymity or performance effects based on what we've seen so far."

Specifically, the hackers were targeting "specialized servers in the network called directory authorities, [which] help Tor clients learn the list of relays that make up the Tor network," Tor said. As of Dec. 28, though, everything was "quiet," according to Tor.

One group that is not a fan of Lizard Squad's attacks on Tor? Anonymous.

Meanwhile, while he seemed fairly nonchalant about the massive attacks, "Ryan Cleary" did apologize for the August attack on American Airlines flight No. 362, carrying Sony Online Entertainment President John

Smedley.

"Only time I think we went a bit too far was the American Airlines incident," he told the Post. "[W]e accidentally got some F-16s to escort John Smedley's plane. [T]hat was going a bit overboard."

Easy Access to Gmail Reportedly Blocked in China

A simple access to Google s e mail service Gmail has been reportedly blocked in China for a while.

In accordance to BBC, locals stated that they re nonetheless in a position to use third-social gathering apps like Microsoft Outlook. Nevertheless, utilizing Gmail by way of Google s website has been unattainable for some time.

Google knowledge signifies that such visitors acquired even worse on Friday and has remained stagnant since.

Google officers stated that there was no challenge referred to as but with the corporate s provision of Gmail.

Meadows, a spokesman for Google Asia Pacific stated that there was nothing flawed on their finish so far as technical points have been involved.

Jeremy Goldkorn, founding father of Beijing-based mostly media tracker Danwei stated that the Chinese language authorities has been aggressive about its web sovereignty and constructive about censorship of web.

Nevertheless, Chinese language authorities has neither denied nor confirmed that the difficulty was a results of recent restrictions.

Electronic Eavesdropping: NSA Reports on Its Privacy Violations

The National Security Agency has a lot to keep track of all those electronic communications and other signals, mostly innocuous but some of which are critical to national security, collectively known as signals intelligence or SIGINT.

In the post-9/11 world of terrorist threats, unconventional war, and rapidly advancing technology, sorting through and making sense of all that SIGINT becomes increasingly critical.

So does protecting the civil liberties of individual Americans, whose private and personal information from cell phone records to email communication may get vacuumed up (or specifically targeted) in the NSA s massive electronic spying efforts.

Recommended: How well do you know the world of spying? Take our CIA and NSA quiz.

On Christmas Eve, the NSA released a report on privacy violations from 2001 through the middle of 2013. It was required to by a Freedom of

Information lawsuit brought by the American Civil Liberties Union (ACLU).

The NSA release, which consists of its regular reports to the President s Intelligence Oversight Board, is heavily redacted. Reports show data on Americans being e-mailed to unauthorized recipients, stored in unsecured computers, and retained after it was supposed to be destroyed, according to documents cited by Bloomberg News.

Some incidents involved deliberate misuse of government surveillance, the Wall Street Journal notes. In 2009, a US Army sergeant used an NSA system to target his wife, also a soldier, leading to punishment including reduction in rank to specialist. In another instance, an analyst in late 2011 reported that, during the past two or three years, she had searched her spouse s personal telephone directory without his knowledge to obtain names and telephone numbers for targeting.

The NSA contends that "the vast majority of compliance incidents involve unintentional technical or human error.

"In the very few cases that involve the intentional misuse of a signals intelligence system, a thorough investigation is completed, the results are reported to the [Intelligence Oversight Board] and the Department of Justice as required, and appropriate disciplinary or administrative action is taken," the NSA said.

"These materials show, over a sustained period of time, the depth and rigor of NSA s commitment to compliance," the agency said in a statement. "By emphasizing accountability across all levels of the enterprise, and transparently reporting errors and violations to outside oversight authorities, NSA protects privacy and civil liberties while safeguarding the nation and our allies."

The revelation that the spying agency had been collecting and storing domestic phone records since shortly after the terrorist attacks of Sept. 11, 2001, was among the most significant by Edward Snowden, a former agency network administrator who turned over secret NSA documents to journalists. The agency collects only so-called metadata numbers called, not names and not the content of conversations. But the specter of the intelligence agency holding domestic calling records was deeply disquieting to many Americans.

The Senate last month blocked a bill to end bulk collection of Americans' phone records by the NSA. Voting was largely along party lines, with most Democrats supporting the bill and most Republicans voting against it.

The legislation would have ended the NSA's collection of domestic calling records, instead requiring the agency to obtain a court order each time it wanted to analyze the records in terrorism cases, and query records held by the telephone companies. In many cases the companies store the records for 18 months.
Patrick Toomey, a staff attorney with the ACLU's National Security Project, told news agencies the new documents "shed more light on how these spying activities impact Americans, and how the NSA has misused the information it collects.

They show an urgent need for greater oversight by all three branches of government, Mr. Toomey said.

Republicans Plan To Push Back Against Net Neutrality in 2015

Republicans in Congress say they plan to oppose any efforts by the Federal Communications Commission to install net-neutrality rules that demand internet service providers treat all online traffic equally.

Republicans in Congress say they plan to oppose any efforts by the Federal Communications Commission (FCC) to install net neutrality rules that demand internet service providers (ISPs) treat all online traffic equally.

The FCC is expected to announce in early 2015 new rules for ISPs that will hue close to President Barack Obama’s plea for broadband service to be treated like a utility, and for web traffic to remain on somewhat equal footing, disallowing ISPs to prioritize certain content.

Though the concept of net neutrality what supporters say is a fight for free and open internet has high support among both conservatives and liberals surveyed in recent polls, as pointed out by TechDirt, Republicans have vowed to fight any attempt to bar the likes of Comcast and Verizon from granting preferential treatment to certain online traffic dependent on payment.

Politico reported on Monday that Republicans, who will have a majority in both the US House and Senate come January, plan to act on threats to quash net neutrality.

Republican Sen. John Thune, who is set to lead the Senate Commerce Committee, is considering a bill that would aim to thwart any such rules presented by the FCC.

Thune is very interested in finding a legislative solution to protect the open internet, especially if it means keeping the FCC from imposing public utility regulations, a spokeswoman told Politico.

Meanwhile, Rep. Greg Walden, chair of a telecommunications subcommittee in the House, has said he will hold hearings to cast attention on net neutrality rules, and Rep. Bob Goodlatte, chair of the House Judiciary Committee, said he may seek legislation that would aim to undermine the FCC s net neutrality authority by shifting it to antitrust enforcers, Politico wrote.

Calling any such net neutrality rules a drag on innovation and competition, Republicans in Congress have said they are contemplating legislation to cut FCC funding, Politico reported, and other methods to hamper FCC moves on net neutrality, according to The National Journal.

"Federal control of the internet will restrict our online freedom and leave Americans facing the same horrors that they have experienced with HealthCare.gov," Rep. Marsha Blackburn said earlier this year.

Democrats and other supporters of net neutrality say such moves would allow for the creation of a multi-tier system and fast lanes in which data is delivered to customers at a speed pursuant to the price paid to ISPs by content creators.

 If a party wants to be insistent on being anti-internet equality, that s a bad place to be, said Rep. Anna Eshoo, top Democrat on the House s telecom subcommittee.

Adding to the mix is a Republican plan to address possible changes to the Communications Act, which guides the FCC and its regulation of cable, wireless, and phone companies.

The Communications Act has not been revamped since the mid-1990s, a long way from telecommunications operations of today. Republicans may tie this debate to its net neutrality maneuvers, according to reports.

Each time it has tried to regulate the Internet, the FCC has been overruled by the courts because existing telecommunications laws were written decades ago for a completely different era, the Thune spokeswoman told Politico. The most straightforward approach would be for Congress to update and modernize those laws to take into account technological transformations while not discouraging the private-sector investment and innovation that is critical for consumers and our nation s modern economy.

Senate Democrats, meanwhile, have urged Republicans to avoid linking net neutrality to any reform of the Communications Act.

Adding to the debate are the possible sales of Time Warner Cable and DirecTV to Comcast and AT&T, respectively. Comcast is seeking FCC approval for the $45 billion acquisition of Time Warner, while AT&T wants the okay to buy DirecTV for $48.5 billion.

In was reported in October that FCC Chairman Tom Wheeler was believed to be pursuing a hybrid plan concerning net neutrality that would separate broadband into two distinct services: a retail one, in which consumers would pay broadband providers for Internet access; and a back-end one, in which broadband providers serve as the conduit for websites to distribute content.

In November, Pres. Obama advocated for a plan more in tune with the demands listed in a highly successful petition that garnered more than 105,000 signatures when it was posted on the White House website earlier this year. In both instances, the FCC was urged to reclassify ISPs as common carriers, like utility companies, which would then give the agency distinct regulatory tools to promote net neutrality.

Obama said in a video posted on the official White House website that Wheeler should implement the strongest possible rules to protect net neutrality when the FCC eventually unveils guidelines that will govern the way in which web traffic is delivered to customers by ISPs. The FCC should reclassify consumer broadband service under Title II of the Telecommunications Act, the president suggested, while at the same time forbearing from rate regulation and other provisions less relevant to broadband services.

This is a basic acknowledgment of the services ISPs provide to American homes and businesses, and the straightforward obligations necessary to ensure the network works for everyone not just one or two companies, Obama said.

Shortly after the president weighed in, however, Wheeler fired back with a response in which he said his agency will hear Obama s plea, but with the same regard as the four million or so other comments received by the FCC over the pending rules.

As an independent regulatory agency we will incorporate the president s

submission into the record of the Open Internet proceeding, Wheeler wrote. We welcome comment on it and how it proposes to use Title II of the Communications Act.

Wheeler later said that the FCC has more work to do on the subject and that the reclassification and hybrid approaches before us raise substantive legal questions. We found we would need more time to examine these to ensure that whatever approach is taken, it can withstand any legal challenges it may face.

 We must take the time to get the job done correctly, once and for all, in order to successfully protect consumers and innovators online, Wheeler wrote.

In response to Obama s call for an adherence to net neutrality principles, Sen. Ted Cruz likened any such moves to the GOP s favorite boogeyman, the Affordable Care Act, or Obamacare.

 Net neutrality, Cruz tweeted, is Obamacare for the internet; the internet should not operate at the speed of the government.

A previous attempt by the FCC to install net neutrality rules was rejected by a federal appeals court.

In January, the court said ISPs should be allowed to restrict access to websites and block certain content from customers, depending on how much consumers pay to be connected.

The three-judge panel agreed with Verizon and said the FCC had classified broadband service providers in a manner that excluded ISPs from the anti-blocking and anti-discrimination requirements instilled through the Open Internet Order.

Politician’s Fingerprint ’Cloned From Photos’ by Hacker

A member of the Chaos Computer Club (CCC) hacker network claims to have cloned a thumbprint of a German politician by using commercial software and images taken at a news conference.

Jan Krissler says he replicated the fingerprint of defence minister Ursula von der Leyen using pictures taken with a "standard photo camera".

Mr Krissler had no physical print from Ms von der Leyen.

Fingerprint biometrics are already considered insecure, experts say.

Mr Krissler, also known as Starbug, was speaking at a convention for members of the CCC, a 31-year-old network that claims to be "Europe’s largest association" of hackers.

He told the audience he had obtained a close-up of a photo of Ms von der Leyen’s thumb and had also used other pictures taken at different angles during a press event that the minister had spoken at in October.

Mr Krissler has suggested that "politicians will presumably wear gloves when talking in public" after hearing about his research.

Fingerprint identification is used as a security measure on both Apple and Samsung devices, and was used to identify voters at polling stations in Brazil’s presidential election this year, but it is not considered to be particularly secure, experts say.

"Biometrics that rely on static information like face recognition or fingerprints - it’s not trivial to forge them but most people have accepted that they are not a great form of security because they can be faked," says cybersecurity expert Prof Alan Woodward from Surrey University.

"People are starting to look for things where the biometric is alive - vein recognition in fingers, gait [body motion] analysis - they are also biometrics but they are chosen because the person has to be in possession of them and exhibiting them in real life."

In September this year Barclays bank introduced finger vein recognition for business customers, and the technique is also used at cash machines in Japan and Poland.

Electronics firm Hitachi manufactures a device that reads the unique pattern of veins inside a finger. It only works if the finger is attached to a living person.

Trials in the intensive care unit at Southampton General Hospital in 2013 indicated that vein patterns are not affected by changes to blood pressure.

Google Outs Unpatched Windows 8.1 Vulnerability, and Debate Rages on Both Sides

A Google researcher has disclosed an unpatched vulnerability in Windows 8.1 after Microsoft didn t fix the problem within a 90-day window Google gave its competitor.

The disclosure of the bug on Google s security research website early this week stirred up a debate about whether outing the vulnerability was appropriate.

The bug allows low-level Windows users to become administrators in some cases, but some posters on the Google site said the company should have kept its mouth shut. Google said it was unclear if versions of the Windows OS earlier than 8.1 were affected by the bug.

Automatically disclosing this vulnerability when a deadline is reached with absolutely zero context strikes me as incredibly irresponsible and I d have expected a greater degree of care and maturity from a company like Google, one poster at the Google site wrote.

The vulnerability is your average local privilege escalation vulnerability, the same poster wrote. That s bad and unfortunate, but it s also a fairly typical class of vulnerability, and not in the same class as those that keep people like me up at night patching servers, the poster said. The sad reality is that these sort of vulnerabilities are a dime a dozen on Windows.

Another poster, in what may be a slight overstatement, suggested the

versions of Windows affected are run by billions of computer users. Exposing vulnerabilities like this has far reaching consequences, the poster wrote.

People could get hurt by this and it doesn t bring anyone closer to a solution. When an organization is as big and powerful as [Google], people working there need to think of themselves as stewards of a great power and work to be fair and regulate the harm that can come of misusing this great power when possible.

Was it a secret worth telling?

Other posters praised Google for sticking to a deadline it s had in place since it launched its Project Zero bug-tracking team last July. No one is done any good by keeping it secret, one poster wrote. By exposing the [vulnerability] they allow those billions who may be running vulnerable systems to be aware of the threat to their own security and take countermeasures. A patch isn t the only way to mitigate the issue. Given the nature of this vulnerability, there are other steps administrators can take to start protecting their vulnerable systems while they await a patch.

Microsoft said in a statement it is working to release a security update to the reported vulnerability. It is important to note that for a would-be attacker to potentially exploit a system, they would first need to have valid logon credentials and be able to log on locally to a targeted machine, a spokesman said by email. We encourage customers to keep their anti-virus software up to date, install all available security updates and enable the firewall on their computer.

Google, in a statement published on Engadget, defended the release of the vulnerability information.

Google s 90-day deadline for fixing bug is the result of many years of careful consideration and industry-wide discussions about vulnerability remediation, the company said. Security researchers have been using roughly the same disclosure principles for the past 13 years ... and we think that our disclosure principles need to evolve with the changing infosec ecosystem. In other words, as threats change, so should our disclosure policy.

Google will monitor the effects of its policy closely, the company added. We want our decisions here to be data driven, and we re constantly seeking improvements that will benefit user security, the company added. We re happy to say that initial results have shown that the majority of the bugs that we have reported under the disclosure deadline get fixed under deadline, which is a testament to the hard work of the vendors.

Microsoft And Yahoo Confirm Search Outages

Microsoft s search engine Bing.com and other sites, including live.com, suffered a brief outage of somewhere around 20 minutes today, give or take, according to reports on Twitter and other website-monitoring services. While Bing.com and others have since returned (in fact, while we were reaching out for comment on the outage), we noticed also that Yahoo s search service (powered by Bing) at search.yahoo.com is currently down, as well. We re reaching out to see if there s any

explanation being provided for the outages.

When you perform a web search from Yahoo.com, you re redirected to search.yahoo.com, and this has only been returning a blank page or, more recently, an error message, instead of search results.

In Bing s case, the site was not resolving at all, though some report seeing the default IIS homepage instead. The website-monitoring service IsItDownRightNow also confirmed that the site was offline for a brief period today.

Some reported that other Microsoft domains, including portal.office.com, outlook.com and hotmail, were difficult to reach, too, but we could not confirm this directly. These sites appear functional now, and in some cases, the website-monitoring service showed no disruptions or didn t have data on the referenced domains. However, it does appear that Live.com did experience a brief outage around the same time that Bing.com was down (and Hotmail redirects to Live.com).

Yahoo s search is powered by Microsoft, so it s not surprising to see both search services go down at the same time. However, at the time of writing, Bing.com had returned but Yahoo s search had not.

During the time of the Bing outage, mobile assistants Siri and Cortana, which leverage Bing, were also affected.

We ve reached out to both companies for a further explanation or official response, but comms and PR staff are still working a holiday schedule which means answers could be delayed.

Update, 1/2/15, 3:30 PM ET: Microsoft has confirmed the outage with a brief statement:

> This morning Microsoft experienced a brief, isolated services outage which has now been resolved. Our apologies for any inconvenience.

Update 2, 1/2/15, 4:20 PM ET: Yahoo has also confirmed its outage:

> We are aware that Yahoo Search is unavailable to users. Our engineers are working to restore the service at the earliest.

Microsoft May Soon Replace Internet Explorer With a New Web Browser

Microsoft s Windows 10 operating system will debut with an entirely new web browser code-named Spartan, according to a report citing anonymous sources.

ZDNet s Mary Jo Foley reports that this new browser is a departure from Internet Explorer, the Microsoft browser whose relevance has waned in recent years. According to Foley, it will be a lightweight browser that looks and feels more like the Google Chrome and Mozilla Firefox browsers. But her sources also indicate that Spartan will be offered alongside IE when Windows 10 debuts next year.

With Mozilla Firefox and Google Chrome grabbing so much of the desktop market and Apple Safari, Google Chrome, and Google s Android browser dominating the mobile market Internet Explorer is no longer the force it

once was. There was a time when it handled about over 90 percent of all web traffic on desktop and laptop machines, but according to research outfit Net Applications, its share has now dropped to 58 percent. On mobile, its share is about 2 percent.

Spartan attempts to address both these markets, according to Foley. Windows 10 is designed to run across a wide range of devices, and according to Foley, the new browser will be available on phones and tablets as well as laptops and desktops. It s unclear whether Spartan will run on Android, Apple s iOS, and other operating systems that compete with Windows, but Foley says there s a chance it will.

Under new CEO Satya Nadella, the company realizes that, in the modern world, its software must run on more than just Windows. In March, Microsoft revealed a new version of Microsoft Office for the Apple iPad. In November, it debuted free versions of Word, Excel, and Powerpoint versions for the iPhone. And earlier this month, the company acquired the mobile email startup Acompli, an email client compatible on both iOS and Android mobile operating systems.

Microsoft Could Kill Internet Explorer; New Spartan Browser Coming Soon

Bad News for Internet Explorer fans, if any! Microsoft’s almost 20 years old Web browser with a big blue E sign might soon be a thing of the past.

With the arrival of Windows 10, probably by next fall, Microsoft could come up with its brand new browser that s more similar to Mozilla’s Firefox and Google’s Chrome, but less like Internet Explorer (IE), according to a recent report published by ZDNet.

"Ok so Microsoft is about to launch a new browser that’s not Internet Explorer and will be the default browser in Windows 10," tweeted Thomas Nigro, a Microsoft Student Partner lead and developer of the modern version of VLC.

The browser, codenamed "Spartan," is a "light-weight" browser with extension support, and multiple sources confirm that this new browser isn’t IE12. Instead, Spartan is an entirely new browser that will use Microsoft’s Chakra JavaScript engine and Trident rendering engine (as opposed to WebKit). But Internet Explorer isn’t going away completely.

According to ZDNet’s Mary Jo Foley, Windows 10 will ship with both Internet Explorer 11 and Spartan, though the former is expected to stick around for backwards compatibility only. The new browser will be available for both desktop and mobile devices running Windows 10.

So far it s unclear whether Spartan will be portable on non-Windows systems, such as Android, iOS, or OS X, but if it is actually imitating Chrome and Firefox, two of the most popular browsers out there, the idea isn’t too crazy. The new browser is currently under development.

However, if this new browser doesn’t use Webkit, it will not likely be accepted into Apple’s App store, because Apple requires all "apps that browse the web must use the iOS WebKit framework and WebKit Javascript" according to its app store review guidelines.

What Microsoft will call the new browser is also a mystery at this point,

as ’Spartan’ is just a codename for the project, and there’s no revelations on what it might be called by the company.

Microsoft hasn t provided any details about it but the company is hosting a press event on Jan. 21 in the company’s hometown of Redmond, Washington, where it is expected to provide more details about the consumer version of Windows 10, so perhaps we will know some more about Spartan then.

Yes, U.S. Workers Do Still Need Their Email

The end of email has been foretold many times, but despite these predictions of doom, U.S. workers can t seem to get rid of it.

About six in 10 Internet-using workers in the U.S. list email as very important to doing their jobs, topping the list of most important work tools, according to a survey by the Pew Research Center.

Email trumped the Internet as a whole, which 54 percent called very important, and ranked well above mobile or smartphones [24 percent] as well as social networking sites like Twitter, Facebook and LinkedIn, which only 4 percent of workers found important. Surprisingly, the use of landline phones outranked mobile phone usage: 35 percent of respondents marked landlines as very important.

Despite email users being subject to hack and phishing attacks as well as spam, it continues to be the main digital artery that workers believe is important to their jobs, Pew said. Since taking hold a generation ago, email has not loosened its grip on the American workplace, the research group said.

The analysis in the report released earlier this week is based on an online survey in September of 1,066 adult Internet users over 18. The respondents included 535 adults employed full-time or part-time, forming the base of the report.
Using the Internet does not lead to distractions in the workplace and does not effect productivity, respondents said. Just 7 percent feel their productivity has dropped because of the Internet, email and cell phones, while 46 percent felt more productive, despite critics worrying that digital tools can be a distraction, Pew said.

What s more, more than half of the workers said that Internet, email and cell phones expand the number of people outside of their company they communicate with. And almost 40 percent said the tools allow them more flexibility in the hours they work, while 35 percent said they also started working more hours due to the digital tools.

Meanwhile, employers are starting to change practices regarding employees Internet usage. Just under half of those surveyed said their boss blocks access to some websites, and 46 percent said there are rules about what workers can say or post online. The latter figure more than doubled since Pew began asking about company rules in 2006.

The Sad Internet: 2014 in Review

The Internet is a place of both joyous wonder and corrosive meanness. There are delightful and hilarious memes and GIFs and videos made by GoPro-wearing puppies. And there are nasty troll attacks, flame wars, and outrage galore.

In 2014, however, we noticed a number of projects and sites that don t fit either trope: neither Happy Internet nor Angry Internet.

They suggest, instead, a Sad Internet.

Some manifestations of the Sad Internet make a mockery of the pervasive clichØ of the magical technology that connects us all, builds community, and generally permits the crowd to find and reward the wonderful.

The Sad Internet is a place full of unwatched videos, unliked photographs, unheard music, tweets that no one cared about, and crowdfunding projects that nobody backed.

Join us, if you will, for a tour of the Sad Internet.

The online music service Spotify gets lots of attention for its mind-bogglingly humongous catalog of songs. This year it also got attention for a previously unnoticed footnote to that feature: Millions of those songs have never been listened to by a single Spotify user.

The website Forgotify plumbs Spotify s unheard depths to present you with a random selection from the zero-listen archives. Think of it, my colleague Alyssa Bereznak suggested earlier this year, as the equivalent of scrounging through a Tower Records (RIP) bargain bin.

Indeed, you might discover a hidden gem. Forgotify s motivation seems to be positioned as giving all this unknown music a second chance. Or, you know, a first chance.

Similarly, there s a note of optimism, or at least yearning, in the name of No Likes Yet yet! As a practical matter, the site is designed to let you discover Instagram photos with zero likes.

As I noted in an item about the site earlier this year, it s also designed to prod you to help these lonely photos (of Starbucks cups and unremarkable hotel rooms and so on) with a redeeming like: As you mouse over each image, you see an exhortation to offer some positive reinforcement as you see fit.

Or you can just indulge in the potential schadenfreude of narrowing results to your own circle of Instagram contacts. Or wallow in the self-pity of reviewing your own unliked pictures.

Only fail to connect?If there s a cheerful rationale for Sad Tweets, it escapes me.

The concept: Connect the application to your Twitter account, and it presents you with a lowlights reel of your attempts at sharing that attracted no likes, and no retweets.

In short, it s a graveyard for your most depressing Twitter failures, as my colleague Jason Gilbert put it earlier this year. And despite his (rather depressing!) wish that the service would expand to allow users to peruse other people s sad tweets, for now it remains purely a mechanism for self-loathing.

Petit Tube is a French site launched this year that, according to New Media Rockstars, plays a stream of YouTube videos with zero views. Local advertising and real-estate clips, along with some random baby, figured prominently in my brief and somewhat excruciating exploration of the service. Visitors may vote on what they see: Cette vidØo est bien? or Cette vidØo n est pas bien? (Roughly translated, that means Yay or nay?)

N.M.R. also points out two other low-to-zero-view offerings.

Underviewed scrapes YouTube for the lesser seen, the underviewed, and contends that there are innumerable videos out there waiting to be discovered. And what appears to be a Sad Internet early mover, the Tumblr 0 Views promised the best of the bottom of the barrel although its last post was actually in 2013.

I suppose it is possible that one of these projects might lead to the discovery of an unviewed treasure that subsequently goes viral. But I notice that despite their relative age, the entries on 0 Views remain mired in the land of four-figure view counts, at best. Sad.

The silence of the crowd?Surely Kickstarter has proved itself the source of some of the Internet s most inspiring success stories people raising money for worthy art projects, useful gizmos, and, you know, potato salad parties. Stuff that simply wouldn t have happened without the support of the Internet crowd.

Sadly, that s not always how Kickstarter stories end. And thus, Kickended, a site that collects campaigns launched on the crowdfunding platform that failed to attract a single backer.

I wrote about the site here earlier this year, and strained to find a silver lining: It s a useful, albeit bleak, reality check. Yes, the Internet makes magic and wondrous and unprecedented things occur. But only sometimes, and not for everyone. (Sheesh, what a Gloomy Gus!)

While it s clearly been a big year for the Sad Internet, I need to give full credit to a pioneer of the form: the Tumblr Screenshots of Despair.

Launched back in 2012, it set out to collect a bunch of screenshots illustrating the feelings of desolation that can often accompany social networking and life online, its creator wrote. SO FUN!

Specifically the site collects the accidentally despair-inducing text and imagery often submitted by readers that gets presented to us by the many digital and social-media services we deal with all day.

Oddly, the site is fun, in a dark-humor sort of way. And apparently popular: Its amusingly depressing posts regularly attract tons of likes and reblogs. Which just goes to show that, on the Internet, even sadness can go viral. Yay?

And, finally, there is the Lonely Sculpture, created by artist Tully Arnot. This consists of a silicone finger rigged to a servo motor, so that it bobs up and down, nonstop. Positioned beneath this ever-tapping digit is a smartphone displaying the dating app Tinder.

Tinder, which is one of the least subtle apps in the world, offers a parade of pictures of potential partners who also use the service,

inviting users to signal interest or rejection with a tap or a swipe. The Lonely Sculpture s automated finger is positioned to mindlessly like every single candidate the app presents.

Lonely Sculpture is a reflection of both our desire for human contact, and of the isolating nature of social media networks and online dating, Artnet glumly observes. As we become more and more dependent on technology, the lines between man and machine are blurred.

Alternatively, perhaps one could interpret the piece as pumping a stream of positivity into a digital ecosystem that often seems to be built around the seeking of quantifiable approval.

Then again, even that reading doesn t make it an antidote to a year s worth of online bleakness. It makes this absurd mechanism the perfect mascot for the Sad Internet.

And on that note, hey have a happy New Year, everybody!

=~=~=~=